FEDERAL TRADE COMMISSION

Do Not E-Mail Registry

Meeting

Tuesday, March 9, 2004

11:00 a.m.

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

PARTICIPANTS:

From the Commission:

Julie Bush

Kim Lucas

Colleen Robbins

Dan Salsburg

Morning Session:

Joshua Baer

Hans Peter Brondmo

Trevor Hughes

Lana McGilvray

Peter Mesnik

Margaret Olson

P R O C E E D I N G S

- - - - -

MR. SALSBURG: Today is Tuesday, March 9th. It is 11:00 in the morning. I am Dan Salsburg with the Federal Trade Commission. I am here at the FTC with my colleagues, Colleen Robbins, Julie Bush, and Kim Lucas. We're here with a number of people to talk about a possible National Do Not E-Mail Registry. They will introduce themselves in a few seconds.

This conversation is being recorded and will be transcribed. The statements made today may be cited in our report to Congress pursuant to Section 9 of the CAN-SPAM Act.

Before you all introduce yourselves, I thought I would explain to you a little bit about the process. We are collecting information from as many possible sources as we can -- from consumer groups, from marketers, from list management companies, from law enforcement, from ISPs and others. This is part of that general data collection process.

We met with Trevor Hughes probably about six weeks or so ago?

MR. HUGHES: Right.

MR. SALSBURG: And he offered to come talk with us more and to bring the technologist to help us better understand your perspective on how a Do Not E-Mail List would

or would not be able to work with the businesses that you operate.

We are thrilled that you're here. In the meetings that we have had with other people, we have thrown out possible Registry models and asked them to discuss them and point out any security, privacy, technical, feasibility, and enforcement issues that they see with them. But here, it sounds like you have come prepared with some things that you already want to talk about, and we are game to go with the way that you want to proceed.

MR. HUGHES: Sure. We can definitely follow sort of the structure that we had talked about, and I will share what that is with you, but also, you know, if there are specific things that you would like to cover, by all means we can dive deep on whatever you would like to cover.

MR. SALSBURG: Why don't we start with how you want to proceed, and if you could all, at the table, identify who you are and where you're from, that would be great.

MR. HUGHES: So, why don't I start? And again, I'm Trevor Hughes, I'm the Executive Director of the E-Mail Service Provider Coalition, and we are a coalition of 46 -- not surprisingly -- e-mail service providers.

E-mail service providers are companies that help other organizations deliver e-mail. And our membership really provides services to the full breadth of the U.S.

marketplace. So every organization, from the largest of the Fortune 500 companies delivering e-mail messages to their customers, through the very smallest of Main Street businesses managing very small lists for the people who walk through their door, and they want to receive e-mails from them.

In that position, we actually have a very unique perspective on e-mail space. Depending on who you talk to, we have had some numbers from third-parties who suggest that our membership accounts for 12 percent of total e-mail that is sent around the Web today. And if you take out spam from that equation -- and our members don't send spam; spam is about half the e-mail world -- that suggests that we could be as high as 25 percent of total e-mail sent today in the United States, particularly.

So, we have a very large footprint and a unique view, but a profile that is not necessarily visible in the marketplace all the time. We provide services for the folks that need those services.

And today we have members of our technology committee here at the table, and I will let them each introduce themselves one by one. I will note that Hans Peter Brondmo, from Digital Impact, and Margaret Olson are the co-chairs of our Technology Committee, and they are also the co-authors of the Project Lumos, which is the technological

response to spam that the E-Mail Service Provider Coalition developed last year, and we will take some time to talk about that today, too. So, Josh?

MR. BAER: Great, thank you. My name is Josh Baer. I run Skylist, which is an e-mail service provider. I have been doing e-mail for about 10 years now.

I first got involved when I was back at school at Carnegie Mellon in about 1996 with standards development and with an RFC -- an Internet RFC -- around actually a list unsubscribed header, to help make it easier for -- at the time it was discussion forums, not commercial lists, but it was the same kind of problem. It was people getting put on lists and having difficulty getting off the list. And I was involved in that back then.

Since then, Skylist, you know, is a pretty diverse service provider. We both sell software and also do host clients that send mail through us, and we have got a diverse range of clients, from non-profits and government organizations and dot-coms that, like, send diet information to highly commercial messages that are, you know, working with, often, subscribers, you know, trying to promote different services.

MR. BRONDMO: I'm Hans Peter Brondmo, with Digital Impact, Senior Vice President. I have been in the e-mail marketing space since the mid-1990s. I started with one of

the first companies, called Post Communications. I have been with Digital Impact for the last few years, heading up our futures project, so long-term directional activities, et cetera.

Digital Impact is the largest e-mail service provider in the industry today. We're a public company. And our client base is about 110 companies, virtually all Fortune 1,000. So we send e-mail from -- so if you get an e-mail from Microsoft or from Hewlett Packard, or from The Gap, or from Target, that's all e-mail probably powered by our infrastructure.

And we have approximately 250,000 customer records under management on behalf of our clients today, and as I said, about 110 clients. So we're here with kind of a diverging view here. And what's perhaps interesting about what you're going to hear today is that we represent a small number of very large corporations with very complex internal infrastructures.

And with CAN-SPAM, some of the issues that came up was we operate with lots of internal databases. Just creating consistency among those within the global enterprise has been a big -- you know, interesting challenge.

Margaret has a very different business model, so I think what we can see here today is a very interesting spread. While we represent something -- somewhere on the

order of 250,000 businesses, we send e-mail on behalf of approximately a quarter of million businesses, you know, our footprint is on 100 of those. But again, large ones.

MR. MESNIK: Okay. My name is Peter Mesnik. I am the Founder and Chief Technical Officer for IMN, Inc., also formerly known as iMakeNews. And we are an e-newsletter service provider and I first got started in the e-mail space back in the mid-1990s, when I actually had a product called NetMailer, which was a desktop program used to -- it was called e-mail merge for the Internet, and it was basically the ability to send personalized e-mail, and we sold in retail stores and sold online, and it was a fairly popular product. We got some attention in "Business Week," et cetera.

And then I started IMN in 1998, and our company basically is responsible for e-newsletters and other types of electronic communications for companies such as General Electric, Shell Oil, so a lot of large, corporate customers, and typically more at the departmental level within those organizations.

MS. OLSON: I am Margaret Olson, I am the CTO of Roving Software. We make Constant Contact, which is an e-mail marketing service for small to medium-sized businesses. We have -- our average customer is -- has less than 2,500 names. We have 20,000 of them. We have -- I have been with

Roving since 1997, when we started initially with a desktop application.

So, our customers are sort of the opposite extreme from Hans Peter's, and they are small. They don't have a complex infrastructure. On the other hand, they don't have long lead times for anything they do. You know? They're surprised if they, you know, finish editing something and it doesn't go out in 10 minutes. They don't -- his customers plan their campaigns; my customers' notion of a plan is, "I think I will do it this afternoon."

And prior to being at Roving, most of my background was in distributed computing, dealing with large distributed systems.

MS. MCGILVRAY: I'm Lana McGilvray, I am the Director of Sales and Marketing for Skylist, and the Acting Vice President of Marketing for Unsub Central, which is one of the private sector solutions for suppression.

My background is actually in regulation and deregulation of telco. Before I came to the e-mail space I helped direct research for the Graduate School of Business at Columbia University, to look at how the historical regulation and periods of deregulation affected both the economic space, as well as the sort of the vested interest on all sides. So what's going on right now is intensely interesting to me.

In the e-mail space, I have been working with

Skylist for the past two years, and basically oversee all marketing, best practices, navigating what we're doing with the various coalitions, and what our viewpoints are.

MR. HUGHES: Great. So, a lot of depth around the table in the e-mail space. And that has been one of the great value drivers for the E-Mail Service Provider Coalition, is we have worked in -- worked towards trying to find manageable solutions to solving spam, is that we do have the depth of our members, which is spectacular.

So, let me tell you what we were thinking about talking about today, and then we can jump from there, and see where we end up.

The big message that we want to get into today is that with regards to a Do Not E-Mail List -- and this may surprise you -- we think you probably could build it. The technology exists, and it would cost a fair amount of money, but there are some concerns associated with that, and some things that we want to make sure that you're aware of, and we also want to talk to you about some of the conditions precedent that we think would have to be in place before you got to that -- to a Do Not E-Mail List -- that was effective and meaningful for consumers in the U.S.

So, with regards to that, we would like to take you on a bit of a journey today. We will talk about one of the conditions precedent that we think exists, and that is

authentication. And Hans Peter is going to talk to you about Project Lumos, which is the architecture, the solution that we proposed last year. We think that building identity into e-mail, authentication into e-mail really is something that would have to exist before you could ever get to a Do Not E-Mail List.

The good news is that Project Lumos really did have a strong influence on the marketplace last year -- at least we like to think it did -- and Margaret is going to talk to you about some of the work that is happening, the major ISPs and how they are picking up on this idea of authenticated e-mail. It really has gained some traction in the last three months, and there are some exciting developments there, and we want to share with you sort of those developments.

And that will kind of cover authenticated e-mail for you, and where that is. We thought that Peter could give you our thumbnail sketch as to how Do Not E-Mail systems could be, at a very high level, conceptually designed, and we will talk about two major models, and we will give you some feedback or some thoughts from a very early point as to how we see those.

And then finally, Josh can talk about some of the private sector initiatives that are underway. The CAN-SPAM Act, as it stands today, actually places some fairly heavy burdens on legitimate senders to make sure that they are

managing suppressed lists in an appropriate way under CAN-SPAM. And that requirement under CAN-SPAM has engendered something of a new industry. It has a very strong analogy to mailhouses and the direct marketing world, and Josh will talk to you about that sector. Does that sound good?

MR. SALSBURG: Sounds great.

MR. HUGHES: Excellent. All right. So let's -- let me have Hans Peter tell you about Project Lumos.

MR. BRONDMO: All right. Are you guys familiar with Project Lumos at all?

MR. SALSBURG: Why don't you give us --

MS. ROBBINS: Yes.

MR. SALSBURG: -- background.

MS. ROBBINS: Also for the record.

MR. BRONDMO: Okay, all right. I will give you the headlines, and then, you know, feel free to build on anything.

When we started doing this work -- it's been about a year and change now -- we took a look at the spam space, and we said the way people are solving this problem, we quickly realized, is they are solving it the wrong way. They are sitting on the receiving end, waiting for the spam to arrive, and then trying to guess effectively which ones are spam and which ones aren't.

And whenever you -- and that's, you know, the whole

-- the filters and the -- all these different fancy algorithms. They are doing nothing but looking at the e-mail, trying to determine somehow whether it's spam or not, and then, you know, putting away the stuff that they think is spam, stuff that they don't really know whether it's spam or not, putting in a "bulk" folder, and then you deliver some stuff.

Of course, the problem with guessing is that even if you guess 99 percent of it right, given the volumes of e-mail, 1 percent wrong is pretty bad. And that's where the false positives problem come from, et cetera.

So, we looked at this problem and said, "Look, there is no way for people who have a legitimate reason to send e-mail, whether that's, you know, your mother sending you a message, your colleague sending you a message, a purchase receipt, a legitimate opt-in marketing message, there is no way for those people to assert that they are who they are, stand up and say, “Here is who I am, I have nothing to hide, let me through."

And so, we changed the tables, essentially, and instead of running around chasing the bad guys and sitting back and waiting for the assault, we said what if we stepped up and we said, "Well, what if there was a well-lit, clean place where all the good guys can step forward and say, here is who we are, we're going to be that guy tomorrow and the

next day, we're not going to forge our headers, we're not going to change our identity as we go, we're going to be the same, consistent mailers the whole time.'"

If there was that place, then you could easily treat those guys and anybody who wasn't willing to step forward, you could assume that they might have some other agenda, in which case you could treat them very differently than you treat the guys who step forward into that well-lit, clean part of the Net.

And so, with that as a conceptual backdrop, we developed Project Lumos. Project Lumos really had two pillars. One was identity, which is if you're going to step forward, you need an identity. And an identity needs to be consistent, because -- or persistent. If it's not persistent, then I will change identity every other day, which is what -- the technique the spammers use, and finally will get through.

So, we need persistent identity, or a way of authenticating senders, but then the second part is we also need a history of that sender. We need a performance metric of some sort, or reputation as it has come to be known. Because if you don't have a reputation, it won't be a problem for Yahoo! or AOL or Microsoft, because they get so much mail that they can quickly determine their own reputation.

But for the rest of the network, for the small

domains, for my personal domain, Brondmo.com, I need somewhere to turn to say, you know, "When I get an e-mail from, you know, Roving.com, what's their reputation? Are they working well or are they not?" And I need some trusted body I can turn to to establish whether they work or not.

So, that was the premise, what we set out to do. When we started our discussion, you know, the focus was very much still on filters. It has moved, we think, very, very conclusively at this point to authentication. And Margaret will take you -- give you some more detail on the way we see that space.

But the reason this is -- I think this is -- interesting from a Do Not E-Mail standpoint is if you -- if I can't represent myself securely, in terms of who I am when I send you a message, you can't stop me. I don't care how many lists you put out there.

If I can pretend -- you know, if somebody else can pretend to be Brondmo.com at any given point, then whether I'm good, bad, or ugly doesn't matter. Whether I'm on the list or not doesn't matter, because what somebody will do is just change. If I am trying to send a message, they will just change their identity and get in that way.

And as you well know, I'm sure, the SMTP, the actual protocols for mail today are completely insecure. I've been on mail since e-mail -- and on the Internet --

since 1982, and you know, back then nobody really thought about these problems, right? As it has evolved over time, SMTP, or the infrastructure, has become insecure. Hence, we need this notion of authentication.

So, what I want to talk about briefly -- and setting the stage here -- is what we think about as a -- in terms of an architecture of accountability. Because at the end of the day, we create that well-lit place where people can step into the middle of the room, what we have created is a place where you can hold people accountable.

And the whole notion here we're trying to accomplish is accountability at the network level. We are trying to hold people accountable at this end, monitor, create a history, create a reputation over time, and that allows you to implement accountability.

So, if you look at what an architecture of accountability looks like, it has three -- arguably, four -- components. The first component is authentication, and that's what you will hear a little bit more about. But you need to know that I am who I say I am.

But all you know when I say that is that I am sending you a mail from Brondmo.com. You don't know whether Brondmo.com is bad or good, you just know that nobody else is faking it; I'm Brondmo.com. That's all you know. That's all the existing proposals provide.

But the next level on top of that is you now need to say -- okay, so if I'm Yahoo! and I'm receiving a mail from Brondmo.com, right, I see a lot of Brondmo.com's mail, I know whether he sends high volume or not. So I can determine whether to let him through or not.

But if I am, you know, a small university, .edu, I am only getting 10, 15, 100 mails from Brondmo.com, and I don't know whether he's a spammer or not. So that's where I need piece number two, which is I need accreditation. Brondmo.com needs to go and be able to accredit his domain, or credit his sending practices such that the rest of the network can see and move and go to those accreditation services and determine whether Brondmo.com is, in fact, legitimate or not.

So, on top of accreditation, you then have reputation. So what I am sending -- you receive an e-mail from Brondmo.com. You go out and you say, "Okay, is this guy for real or not? Yes, he has been accredited with a trusted accreditation service, he's for real." Now you ask when he starts sending e-mail, you start -- you ask, "Does he have a reputation?"

And if he has a reputation and it's a good reputation, you let his mail through. If he doesn't, you don't let his mail through.

Now, this infrastructure is starting to evolve.

The base line is authentication. We need authentication. Layer two is accreditation. That's starting to happen. You have got guys like Brightmail and others, that are kind of looking at providing service, you're looking at providing accreditation services. On top of that, they're also providing reputation services.

And on the last level, on top of that, once you have all those pieces in place, now you can actually talk real enforcement. And so due process, and kind of the legal structure on top of that, so you can actually enforce.

So, the architecture of accountability starts with authentication, then looks at accreditation, once you have an authentication mechanism, reputation on top of that, and then finally, enforcement.

So, in wrapping it up, the reason this is interesting from a Do Not E-Mail standpoint is that as you will hear through the conversation a little bit, there are really two different models for accreditation. And here we will talk to you a little bit about a distributed model and a centralized model.

In a distributed model, and with CAN-SPAM as a backdrop, it actually turns out that with the authentication you will be seeing today, and the accreditation services on top of that, you have a de facto Do Not E-Mail List evolving organically in the marketplace today.

Because it will become increasingly difficult for somebody to send mail if they are not authenticated and they are not accredited. And if I am accredited, I might be accredited to send purchase receipts only. I might be accredited to send personal e-mail only. I might be accredited to send commercial e-mail of different classes, different types.

And if you can trust my accreditation service -- and my accreditation service is a commercial service available on the network, and there are competing services -- now you can also trust the fact that I will only send a certain type of e-mail. Because if I don't, I will lose my accreditation, and I won't be able to get my mail delivered.

So, the commercial marketplace, I think, is in a key position right now to develop some very interesting services and technology capabilities that will, in fact, allow for a de facto enforcement of the CAN-SPAM, you know, suppression and unsubscribe provisions, and we will effectively have a Do Not E-Mail List.

So, with that, I think I'm going to hand it over so we can kind of now drill down one level, talk a little bit about what, in fact, is happening specifically with authentications, since that's where all the activity is going on right now -- we've had a lot of dialogue with the ISPs -- but then also look at this model of a centralized, which is

kind of what you guys have called for, the way we look at it, kind of framed it, versus a decentralized, which is kind of where the market model under this architecture, for example --

MR. HUGHES: And let me just ask. Has Microsoft come in and talked about Caller ID or CSRI, or Yahoo! come in and talked about Domain Keys?

MR. SALSBURG: They have not yet, but we are communicating with them.

MR. HUGHES: Okay. Good. Well, if you need any help in terms of what questions to put --

(Laughter.)

MS. OLSON: Yes, because we have spent a great deal of time looking at the authentication proposals, because they are critical to getting any kind of accountable e-mail. And of course, including actually enforcing a Do Not E-Mail List so that you know who has actually sent.

There are about three what I would call current proposals that have, you know, widespread support and have been -- about which there have been active conversations across many parts of the industry. We actually hosted a meeting in January in which we had ISPs and some of the mail vendors and ourselves talking about authentication and how you might do it.

All of the current proposals involve registering

information and about who you are, and the name service that is current -- the DNS, which is how you get -- find a web site because that is an existing deployed infrastructure, and it's, you know, it's attractive.

They are all -- the three are SPF, which is an open source initiative, Domain Keys, which is from Yahoo!, and Caller ID, which is from Microsoft. They all authenticate slightly different things. So there is both a technical discussion and what I would call a policy discussion, which is what should you be authenticating?

Most of the discussion today has been technical, and I will just sort of give you a really high-level description of the differences between -- there are really two parts to sending a piece of e-mail.

One is making the connection and making -- and something called the envelope, which is basically -- it's just like the envelope from when you send a piece of postal mail. It tells you, "Where should I send this back to," right?

And then there is the "from" address, which is the one that you see when you open the letter, right? So you could have a return address on your envelope that's completely different from what's there when you open it. SPF authenticates that envelope return address.

This is really important in preventing certain

kinds of -- primarily network -- abuse. To consumers, it's pretty uninteresting, because they don't really care, you know, who handles return mail. Caller ID authenticates that -- what the consumer sees. And Domain Keys also authenticates primarily the "from," and it authenticates the headers, as a group.

All these are doing this on a domain level. That is, what they're looking at is what domain it came from, and basically saying the domain is responsible for what emanates from it, which I think everybody in the industry thinks perfectly reasonable requirement to put on somebody who is running a domain.

Caller ID is probably the most sophisticated of the proposals at the moment, in that it integrates a mechanism for making a statement about your policy. So it integrates mechanisms for saying things such as -- that Hans Peter outlined about what kind of mail you send and how much mail you send.

There are -- Caller ID is also the most complicated to implement, just because it is richer. Domain Keys requires an encryption infrastructure, which some people feel -- well, people have opinions about it.

At this point, the technical discussions about the three proposals, I would say, are arguments about what is included and arguments about what is actually deployed on the

Internet and how people send mail. Because the mailing infrastructure is more complicated than most people realize. The variety of ways people send mail is very wide.

So, at this point, what we are doing, and as part of the Technology Committee -- and many other senders are doing -- is starting to publish authentication records in these protocols, because that is how we're going to find out what actually works. You can have a debate about the technical matter all day long, but until you actually test something, you don't know.

My personal feeling is that we will see something emerge some time within the next six to nine months, after a broad cross-section of the sending community has had the opportunity to figure out how to publish. The protocols are all conceptually simple, but that doesn't mean it’s a matter of moments to actually do it.

And the receive-side community has similarly had a chance to evaluate what they actually get, whether the mail that purports to be authenticated does successfully authenticate, and the sender, you know, thinks that the receiver got the right answer.

So, that is pretty much the state of the authentication space. I think we are all very encouraged, because it's clear that although there are probably flaws in these as they stand today, the -- you know, the broad

industry has worked out a general approach that is going to work, and we will wind up with authentication.

MR. BRONDMO: Can I just add one thing to that, which is I think that -- just in summary conclusion, and I don't know if you will agree with this -- but 12 months from now, e-mail will be authenticated.

MR. HUGHES: Yes.

MS. OLSON: Yes.

MR. BRONDMO: Every one of our companies, all 250,000 we send for, every e-mail we send out will be authenticated. So 20 percent of the network right there, you look at the ISPs, the big 10 ISPs representing 60 percent of the network traffic, so a total of --

MR. HUGHES: Legitimate network traffic.

MR. BRONDMO: Of legitimate network traffic.

PARTICIPANT: Right, right, right.

MR. BRONDMO: Sixty to seventy percent of the network infrastructure in twelve months will have authenticated e-mail of some form.

So, authenticated e-mail, I think we are kind of taking that as a given. Now, we don't know exactly which one, and when they're going to evolve, but we're taking it as a given that within 6 to 12 months, the infrastructure will move towards authentication at the domain level, domain authentication for e-mail.

MR. HUGHES: And just to reinforce, the E-mail Service Provider Coalition is working with Microsoft and Domain Keys and engaged in conversations with them, and in some cases we're actually getting ready to start beta testing, because we represent a spectacular test bed for it. I mean, we do represent a big swath of the sending side of the e-mail world.

So, those efforts are aggressively moving forward right now.

MR. SALSBURG: How will ISPs use authentication? Is it just through filters, to --

MR. HUGHES: The big picture here is that authenticated e-mail doesn't necessarily solve for spam. But what it does do is it allows ISPs to be more aggressive with unauthenticated e-mail.

So, if you can hold someone accountable when they come through with a piece of authenticated e-mail, it's that much easier to identify them, to find them, and to switch them off the next time they try and use your system or actually go after them under the CAN-SPAM Act, or otherwise.

Then you can let that e-mail through with much more confidence. For unauthenticated e-mail, you can turn up the dials on some of the other solutions that are in the space today, whether it's challenge response, whether it's filters, whatever it might be, you can really start to turn up the

dials on the unauthenticated e-mail that is otherwise coming through your system.

MR. SALSBURG: How would these three proposals that are out there affect personal e-mail? Would they be deemed authenticated, or unauthenticated?

MS. OLSON: Well, presumably, your personal e-mail would go through, say, Yahoo!, right? So, Yahoo! is essentially authenticating on your behalf, and they might be making an accreditation statement like "Our senders only send 100 messages a day," right? Because they control the mail server and the interface, so they can completely control that. So, you, as an individual, wouldn't even notice, you know, that anything in your world had changed. And the domain --

MR. BRONDMO: Except there is less spam in your inbox.

MS. OLSON: Except there is less spam in there, except that there is less spam in your inbox. And the anonymity issue gets addressed the same way, because I can run an anonymizing surface, where I send out -- you know, one of the things I say is I only let people send 100 messages a day and you, subscriber, I will never reveal your identity unless someone shows up with a subpoena.

So that kind of addresses the free speech, anonymous e-mail issues which are very, very important to

certain segments of, particularly, the technical community.

MR. BRONDMO: There are some complexities here, in terms of being used interchangeably. So when we talk about identity, for instance, in this context we're really talking about domain-level identity, not the 10 of us around the table as individuals.

MR. HUGHES: User level?

MR. BRONDMO: So it's not user level identity, it's domain level identity. You talk about authentication, again, it's domain-level authentication for purpose of these conversations, not individual authentication.

So, the really important -- the importance of accountability here has to do with those running the infrastructure. And in many cases, as Margaret was just saying, the end user won't even see a difference. Those running the infrastructure can now hold each other accountable for what they do and how they operate on the network.

But that -- and they, in turn, the operators, have to hold their users accountable. So we, as ESPs, have to hold our users accountable -- 20,000 customers or 100, if one of our customers decides to do something that -- one of our clients decides to do something that their customer considers spam, we would opt them off our network, because our reputation, our collective reputation, will suffer.

So, there is accountability being built in, because you can't hide who you are anymore. And therefore, if you misbehave, you know, the next time you try it, you will be identified.

MR. HUGHES: And let me make sure we thread this back to Do Not E-Mail. The last time we were in we talked about one of the major policy concerns that we have associated with Do Not E-Mail today is whether it would be effective.

Now, the good guys that -- like the folks around this table -- that are already complying with CAN-SPAM and are actually already using opt-in or consent-based processes for delivering e-mail would participate. But the spammers wouldn't. We know that the spammers would not.

In order to have any effective enforcement under a Do Not E-Mail List, you would need to start to have baked into e-mail some mechanism for authenticating or identifying who is sending e-mail. And this is, again, one of those conditions precedent to making a Do Not E-Mail List effective. So that's why we're spending so much time taking you through it.

MR. BAER: One other quick point is that all these techniques that we're talking about are designed to help deal with today's existing solutions. So right now, the easiest tool, and the most effective one that a lot of ISPs have --

especially smaller ones have -- for blocking mail is really just looking at volume.

And they are very -- I would call them dumb -- filters. "You're sending this much mail in this much time in this place, we're going to block you." And what's cool is this allows us to bypass those things for legitimate people that have reasons to send larger amounts of mail. And if you want to send a large amount of mail, you need to go through these processes.

If you're an end user sending individual e-mails, the filters are much less likely to pick up on you because they're coming in as individual e-mails. So it's really only -- you know, this is both from a cost effective and computation effective, this is the easiest way for ISPs to block spam.

And when they were saying they could turn up the dial, that's what they meant. They would get more aggressive about blocking volume mail from people they don't know, and still not be so aggressive about the individual mail.

MR. SALSBURG: About six months or so ago ISPs saw spammers' tactics shifting away from the use of open relays to the use of compromised proxies. Would a zombie drone be authenticated under any of these proposals?

MR. HUGHES: It could be authenticated, but you would be able to pick up the fact that it's a zombie drone

pretty quickly and have it switched off pretty quickly.

PARTICIPANT: They would lose their accreditation, their reputation.

MR. HUGHES: Right. They lose their ability to sort of --

MR. SALSBURG: The reputational end of it -- authentication alone would --

MS. OLSON: Right --

MR. HUGHES: In order to get to reputation, you have got to have the authentication in order to know where it's coming from.

MS. OLSON: And actually, most of the drones today are sending -- they are not sending through the ISP's mail servers. Most of them are sending -- essentially, operating a mail server on the drone. So it would be difficult to authenticate --

MR. HUGHES: This is a bit off track, but I will send you to a web site to see exactly this type of thing in place. Atriks.com -- we're pretty sure that it's that notorious spammer out of Manchester, New Hampshire -- and I forget his name right now -- has set up a distributed spamming model where he's actually paying people for CPU time to serve as spam drones for him. So, go visit Atriks.com. I think he's paying $.25 per CPU hour, and it's fascinating to see.

MR. BRONDMO: This might be getting into a little too much technical detail here, but in recent discussions among the ISPs who are primarily driving the authentication work, one of the things that's come up is opening a separate port on the mail servers such that any time you send legitimate mail -- if I'm an Earthlink subscriber, say any time I send legitimate mail I actually have to connect into my Earthlink mail server to send mail.

So now when I go to my hotel here, all I do is I just send mail from the hotel, and if the hotel left the mail server open, I can send as much mail as I want, pretending to be from Earthlink. That wouldn't work any more, it would break under these authentication proposals, which is -- and the same technique that I'm using at my hotel is the technique that these droners use.

But if they open up this new -- you know, sort of a whole new channel of communication, and that channel would then authenticate the connection, and you would then be able to send through Earthlink's mail servers and only those mail servers would be authenticated.

So it does -- there are changes and shifts in the way the configurations happen that will have to evolve. But once the big guy starts doing that, I think there will be enough volume of authenticated mail that everybody will kind of say, "Well, if I do this too, I will reap the following

benefits," and I think we will see, you know, the effect.

MR. HUGHES: So, assuming authentication, we think that a Do Not E-Mail system could be possible, but we really don't think that it's necessary -- why don't we have Peter talk to you about -- you know, it will be interesting to see if this matches to what you have seen so far in responses and in conversations. We will talk about some of the sort of broad architectures under which these could live.

MR. MESNIK: Okay. So, when we spend some time thinking about this, I think that there are two approaches that I sort of see taking here.

Initially, and the most obvious one would be a centralized global list, sort of what the easy -- you know, when you sort of think about the problems and say, "If I have a Do Not Call, Do Not E-Mail list," right? But there are a lot of technical problems that can be -- the undertaking is very large.

When we think about just the amount of e-mail addresses that are out there, in comparison to phone numbers, the amount of e-mails that each individual may have on an active basis, and also, if you think about the number of times you would change jobs and addresses that sort of slip through that process. Our estimates -- I think we accounted for 250 million?

MS. OLSON: Three hundred.

MR. MESNIK: Three hundred million? We think it's not unreasonable to think a system should accommodate a billion e-mail addresses over time, because within a period of time if you don't have a very aggressive method of trying to figure out how to clean that up -- I mean, because there are a lot of e-mail accounts, who knows if they're really still effective or not.

So, there are issues related to the scope of the size of the database. Also creating, in a sense, managed by a central authority. That's one single point of failure that you're actually creating, a very large single point of failure that could -- whether it's a security issue or whether it's a technology issue, it could bring e-mail communications to a halt because it's so centralized.

And there are some benefits to that, of course, because it's updated frequently, and so it can be very current. And it can be under control, centralized control, but it -- there is just computational power you would need and the end requirements such as a type of authority would be very significant.

There may be some ways to get around it. You could use some type of distribution, some type of content distribution, like a model where you might have distributed sort of -- to a certain extent. But generally, you know, as a centralizing model, those are some of the issues.

The distributed concept is actually -- we think is a much more novel way to be thinking about this. And there are ways of thinking about it where it's not necessarily just one, big global list.

You could decentralize -- and really start to take advantage of some of the existing things that we are all doing today, and then build on top of that to put it all together. And what you could end up with is the fact that companies today are building their own opt-out lists or Do Not E-Mail Lists, and that's what they're doing.

By the nature of the regulation and the environment out there, they're all doing that. E-mail service providers are doing it, companies are doing that. And in this model, you could -- so, therefore, each of the entities, senders, could be responsible for their own version of or, in their scope, their Do Not E-Mail List.

And a centralized clearinghouse could be used to forward -- to be a centralized place where consumers could come, organized by a central authority, but these consumers could come and provide their request to be opted-out from various communications from various types of senders, and that information could then be disseminated to those senders for inclusion in their opt-out lists, and a return receipt could then be sent to the central authority.

So now, there is a record and there is a large

list, but there isn't any -- all of the various lists are held internally in security of each of those within the network, and the master list is a great record of the fact that the opt-out request had been made, or the fact that you don't want to be included on a Do Not E-Mail List, and can then be used for authentication and identity, and all these other structures in place to effectively provide sort of a legal enforcement framework, and also a methodology for helping support consumers and their desire to receive e-mail.

MS. ROBBINS: Is this presuming that every single marketer would actually have an opt-out list?

MR. MESNIK: That would -- yes, that there would be a certain level of requirement that either the marketer or through their provider, there would be someone maintaining that list. So wherever I'm sending mail, if I'm General Electric and I'm using IMN to send all of my outgoing mail, I can be utilizing IMN's opt-out Do Not E-Mail service.

So, IMN is responsible for controlling and holding on to the Do Not E-Mail Lists for all of our constituents and acknowledging and sending the return receipts to the central authority.

MS. OLSON: And I think it's worth mentioning that all e-mail marketers currently have opt-out lists.

PARTICIPANT: Right.

MS. OLSON: Right? It's --

PARTICIPANT: A requirement now, the law.

MS. OLSON: It's also a requirement of just good practices. So everybody --

MR. HUGHES: The symmetry here is that under CAN-SPAM today, senders -- meaning advertisers -- have to maintain an unsubscribe list, a suppress list we would call it in this space. And that process is being built as we speak.

In fact, most organizations already have it in place, and Josh is going to tell you about some of the private sector solutions that are emerging to help process that.

As a result, on a sender-by-sender basis, on a sort of distributed model, which is really what the Internet is, we have many opt-out lists all over the country across legitimate senders right now.

So, we are, in effect, maintaining a Do Not E-Mail service under CAN-SPAM because of CAN-SPAM as it stands today. It's distributed, which is significantly safer, from a security perspective, significantly less expensive, because it's not centralized and monolithic, and it doesn't create that single point of failure, which, whether from a security or a technological perspective, is problematic, we think.

But it is a de facto Do Not E-Mail List that's occurring today.

MR. SALSBURG: So, let's say I'm an AOL customer, and I register with the central authority that I don't want to get spam. What then happens to my e-mail address? Who does it get disseminated to?

MR. BRONDMO: I think there is an important piece that's missing that we're kind of taking for granted here, and I just wanted to clarify, which is we are making some assumptions around accreditation and reputation here, which is if you maintain your own unsub list you won't be able to operate effectively.

So the assumption is that there will be built-in accountability at the network level, so that when we talk about the distributed model, we have got authentication so we know who is sending. Now what we need, and what we're starting to see in the market place, are the evolution of interpretation services.

So, if, you know, as was pointed out, through CAN-SPAM, you know, everybody -- I mean, we have had suppression lists since day one. I mean, you have things like blacklists to deal with in the past, and you had probes, and you had all kinds of reasons you wanted to suppress since the beginning of time in this space.

So, what we're saying is that's now become -- everybody has to have one, because you have to honor unsub requests, because of CAN-SPAM today whether you want to or

not. With authentication, and then with the reputation services to determine whether you are, in fact, behaving as you are stating or not, you will get accountability built into the system, and you will get those who don't unsub and honor unsubs, they will be held accountable by the network. They will be dropped out.

(Several people speak simultaneously.)

MS. ROBBINS: -- a lot of illegitimate marketers who are not complying.

PARTICIPANT: And that would become apparent immediately through the information services provided.

MS. ROBBINS: Right.

MR. HUGHES: Let me explain a market discipline factor that our members live every single day, and in many ways is as compelling, if not more compelling, than sort of federal oversight for the CAN-SPAM Act, and that is deliverability.

All of the folks at this table, all of our 46 members live and die on a daily basis by how the ISPs handle their mail coming through their systems. And that is correlated almost directly to their success as an e-mail service provider.

Clients and customers, as they are looking for e-mail service providers, really compare them based on how much of their mail is going to get delivered. So, an e-mail

service provider or large sender has an enormous incentive to make sure that they are processing unsubs appropriately, that they are not getting complaints, that their e-mail is coming through in a clean way. Because if they don't -- AOL, Microsoft, Yahoo!, ISPs generally, the tens of thousands of mail gateways that are out there -- will start to block their e-mail.

So, on a day-to-day basis, the legitimate players in the space are living on a pretty strict discipline of making sure their e-mail is clean. And that discipline has led to suppress lists existing, essentially since the start of time. But now, under CAN-SPAM, those suppress lists really have sort of a legal mantel to sit upon.

PARTICIPANT: Also, the Do Not E-Mail List really supports very clearly the principles of the CAN-SPAM Act. So it really is a good match.

MR. SALSBURG: Here is a description of how this model would work. I register my --

MR. HUGHES: Actually --

(Several people speak simultaneously.)

THE REPORTER: I can only get one person at a time.

MR. BAER: Okay, sure. I think I can address that question. And what I would like, if it's okay with you, is we will quickly just look at where have things been, and then what happened as soon as CAN-SPAM happened, and where are

they going right now, regardless of other issues.

So, where have things been? Real quickly, like Hans Peter said, this isn't a new concept. Every e-mail company has a suppression list. What's a little bit new -- and maybe pushing back to advertisers -- that now the advertisers feel like they need to maintain a suppression list, but they turn around and to their partners and the same people that maintain these global suppression lists to maintain those for them.

Even taking a step further back, none of this is new if you look to the same model of the offline work, where there is, you know, suppression lists and they deal with these same types of issues, and there is one e-mail house -- this is a very familiar model to a lot of them. I wish it was a little bit more familiar -- I'm still getting exposed to it, but you know, lots of people have the existing industry problems that we have solved.

Before CAN-SPAM, responsible marketers and advertisers were in on this. I could name a couple of companies that were passing around suppression lists that we had to deal with that our customers would want to work with, and we need to take their suppression list and process it. It was hard to do, they didn't do a very good job of it, it was a lot of work, it cost them a lot of money.

So, CAN-SPAM came out, and basically we're finding

people in one of three modes. They're in denial, they say, "No, it couldn't possibly be that, we don't have to do that, it doesn't make any sense. No, it's too much work," and there are people that are doing that.

There are lots of companies -- and all the biggest ones that we all work with are making e-mail lists and they are maintaining them themselves and they are looking to their partners to help them do that.

And then there are very large companies that are not sending e-mail right now, until they figure this out. They are kind of confused, then. They don't really know what the interpretation of -- and they are losing a lot of money every day.

One thing that has become really clear is that trust is a huge issue, because people are getting -- you know, trusting to manage their lists. And one rule that's involved that I have been involved with is kind of a third-party central authority to act as that trusted party.

And the other part of it that's interesting is it's a multi-channel problem. CAN-SPAM doesn't regulate bulk e-mail, it regulates all commercial e-mail. So it's going to technically -- at least the way we're reading it -- it would apply to "refer friends" that are sent and salespeople -- different types of notifications coming off of large web sites, option notifications, all kinds of things might tie

into that. It becomes a really complicated problem that's hard to solve.

So, how would something like a distributed model work? Well, one of the key components is you're making this assumption that we're going to follow CAN-SPAM and go by its guidelines. Say that the thing you're unsubscribing from is not just -- I'm not going to get any e-mail ever, which may have its own confusing implications of its own and be hard to really achieve, but I'm not going to get an e-mail from this person I know, or this authenticated entity.

And a lot of people that we have -- both on the consumer end and on the marketing end -- feel that if consumers felt they had this confidence that if I really click unsubscribe from Wal-Mart I'm not going to get any more e-mail from Wal-Mart, that would really help them feel good about the spam problem, feel like they're addressing it, and able to get the mail out of their box.

And so, the way it would work is -- and they way we're implementing it now -- is we maintain -- you know, we have a centralized service that maintains a suppression list for each different advertiser. The advertisers control it, they have access to it, it's their information. They give out keys for different people they want to work with, which allows them to come in and scrub their list on the server in a very secure way.

A lot of the existing solutions out there now, some advertisers are making their own solutions. Most -- every e-mail service provider has a way of providing this -- I would say the e-mail service providers have some good solutions, are fairly secure.

Right now, if you go to Google, and you search for suppression lists and start clicking around, I bet you can download a list of 50,000 e-mail addresses from some company they've unsubscribed that they have got sitting on a web page somewhere.

And there is a lot of those. And that's really insecure. They don't realize that they're actually increasing their liability under CAN-SPAM. That's illegal under CAN-SPAM. You can't -- you have to protect those addresses, and you can't, you know, make it easy for people to get a hold of them.

But people are really just setting up these, like, glorified FTP servers where anybody can come in and just download -- anybody that works with them can come down and get these addresses. And they don't even know if they used it or not. There is no audit or log in, there is no nothing.

So the way the distributed system works is a centralized repository, everybody is trusting it, because everybody is giving their data there, so the list -- they don't want to give that to the advertiser, because it's

digital. Once they give up a copy of it, it's gone. They don't need a list on it any more.

And the advertiser is the one that's liable, they don't want to give their list to the affiliates, who could accidentally -- or for some other reason -- mail it to them.

And so, through a combination of techniques I think you have heard about, like hashes, you're able to one, pass around these encrypted e-mail addresses, and also what's most preferred by most partners we're working with now is actually on the server. So the marketer uploads their list to us, we clean it on the fly, and hand it back to them, and then they've got now a clean list.

And what's cool about that is even for encryption and stuff, they never got any e-mail addresses they didn't already have. And so nobody ever sees any, you know, shares any information. It just gives them the minimal amount to not send the stuff.

The way a distributed model might work -- and there are lots of options about how this could go. We are not -- we don't have the answer, you know, we just have -- we think we have -- a lot of good ideas, and a lot of consumer experience.

But you know, one way it could work is even by Caller ID. In DNS, you've got a record for your domain or your entity that says, "This is who we're working with for

our suppression list, and this is how you access it."

We evolved just like the way the Internet always has, with standards and some common ways for people to interact with those, and be able to work with different suppression lists. And that way, the centralized part becomes just a way of finding the thing you need, and each company is responsible for implementing that on their own, or could be part of a larger centralized service.

There could be three big centralized services that everybody uses, there could be one big centralized service, there could be everybody using their own. That's not really specified by -- you know, we can look at that. Does that help with the question --

MR. MESNIK: If you could envision a central place where someone could go, which could be like the sort of clearinghouse on top of all of this that says how -- you know, you could say, "Well, I don't want to receive any more e-mail from Sears." You might also be able to say, "You know what? I don't want to receive any more e-mail from all the retailers in this category," and the system would -- could, in theory, maybe have some knowledge about that.

But the idea is that there is some way, from the consumer's perspective, that there is one place that they know they can go to submit their e-mail address, which is going to live up to the -- in everyone's minds what they view

a Do Not E-Mail List to be. But the actual implementation is a very modern network-based implementation, but a distributed implementation that will also be much more precise as to what they do and don't want to receive.

Because I think a lot of people will find that if it was a centralized model and didn't have a lot of that intelligence behind it, they would suddenly stop receiving a lot of e-mails that they actually do want. They haven't been able to accurately describe -- the most accurate way to describe it is to say exactly, "This sender, from this sender I don't want it, from this sender I don't want it."

If there is a way of classifying them in some various ways and using their reputation and accreditation to help organize that -- but that seems like a way of envisioning this that may be a little different than, you know --

MR. SALSBURG: Doesn't a distributed model pose some security challenges? You would have --

MR. MESNIK: Actually, I think it's less.

(Several people speak simultaneously.)

MR. BAER: But what's the consequence of one event? It's the very smallest, potentially -- it could be even the suppression list is all hashes, and even if it were compromised, there is nothing you can do --

(Several people speak simultaneously.)

MR. SALSBURG: I am a marketer, and I have my list of, you know, a million e-mail addresses that I want to mail to.

MR. BAER: That you want to mail to?

MR. SALSBURG: I want to mail to. How do I know whether or not they are on --

PARTICIPANT: -- Do Not E-Mail List?

MR. BAER: Well, no, because you're mailing for someone else. You have the List, and you're mailing for an advertiser and so you need to --

MR. SALSBURG: Right. I had no prior communications of any --

(Several people speak simultaneously.)

MR. BAER: At the same time, you have to have previous communication with them. There is no -- you have a contract with them. And some way, or through a third party, you are acting as an agent of theirs. They are going to pay you for what you are doing, so you have some --

MR. SALSBURG: No --

MR. HUGHES: Let me clarify, yes. So do you mean, "I'm Sears and I'm sending to Sears customers," or, "I am" --

MR. SALSBURG: Say I'm Sears and I'm sending to Americans who somehow are not Sears customers.

MR. BAER: Good question. So, fundamentally, what we're talking about is -- and this may be part of what we

mentioned before, what do we want to achieve through this Do Not E-Mail List, you know, what this doesn't do is create -- I think this really raises a question of what we're trying to achieve, opt-in or opt-out, and you know, through CAN-SPAM, it really kind of points to an opt-out model.

And what the Do Not E-Mail List, as one big list, achieves possibly is some way of getting an opt-in model to say, "If I put my name on that list now and suddenly opt-in, I'm not opt-out."

And you know, there are certainly a lot of pros and cons around that issue as well. This doesn't approach it that way. This says, "Sears can e-mail to anybody that didn't have e-mail from Sears."

MS. OLSON: Right. But you actually could do a Do Not E-Mail List in a distributed way if you assume that there is some way of finding out where people who belong to, say, AOL, if there is some way of finding out where my -- where I have registered that I don't want to mail.

And you can envision a lot of different ways of doing that --

MR. MESNIK: Collect a list of people that they could then share with central registry. I mean, the --

MS. OLSON: Or you could just do it the same way you do some of the authentication stuff, you go and you look up AOL's DNS record where is the AOL -- where did AOL users

register -- I will just call them their e-mail preferences. That might be at AOL, it might be at some third party.

So now, you start to break up the list. And when you break up the list, you make it more manageable and more secure, because you don't have everything in one place, and you have something that's -- potentially spreads beyond the United States, which I think is ultimately necessary.

MR. SALSBURG: Are these the same models you are both describing, or are these different variations?

MR. HUGHES: They're all variations, you know, they're flavors.

MS. OLSON: They're flavors, right. You can -- fundamentally, I think we all agree it's totally the sender's responsibility, right? And the question -- these different models really boil down to different technical ways you could implement different definitions of Do Not E-Mail.

You could have a distributed model that was just a very basic definition of Do Not E-Mail, which is "I do not receive e-mail from people I do not have a relationship with," or you could have something more sophisticated, along the way Josh and Peter have it, that allows you to have a more nuanced description for every --

MS. ROBBINS: If I'm a consumer, though.

MS. OLSON: Right.

MS. ROBBINS: And I don't want to say, "Sears, I

don't want mail, Gap I don't want mail," you know, whatever, I could go to this central Registry and say, "I don't want anything."

MS. OLSON: That's right. I guess what I'm saying is --

MS. ROBBINS: And then that's forwarded to every company?

MS. OLSON: What I'm saying is --

MS. ROBBINS: How does that work?

MS. OLSON: You could probably do it if you wanted to do that. In the distributed model you would have some number of people in the suppression list business, which I'm just inventing, right?

And then you would have -- you would go and you would register with them -- with one of them, for example -- and when I want to send I would go through a process very similar to what Josh described. If I wanted to send unsolicited e-mail, very similar to what Josh described, where some hashes of my e-mail addresses are actually stored there, so that the list is scrubbed and then I send.

MS. ROBBINS: But then you get a subset back.

MS. OLSON: You get a subset back. You don't get back --

MS. ROBBINS: But you know --

(Several people speak simultaneously.)

PARTICIPANT: These people on your list don't mail to them.

MS. ROBBINS: Right.

MR. HUGHES: The Colleen@AOL.com was on the --

MS. ROBBINS: But you said you effectively though, have a list of people who don't want mail.

MR. HUGHES: But you had that list already. Say it's 10 people --

MS. ROBBINS: Right, but isn't it more valuable though, now you know you don't want --

MR. HUGHES: I wouldn't say so, no.

PARTICIPANT: Well --

MS. ROBBINS: Well, wouldn't the illegitimate spammer, though --

PARTICIPANT: There is a possibility that --

(Several people speak simultaneously.)

PARTICIPANT: One key distinction, though, is that we're not -- ideally -- we're not storing e-mail addresses, we're storing these hashes. And the hash, you can't get from that hash back to the e-mail address. So there is no risk of it being compromised.

MS. ROBBINS: Except that you could create a sublist, knowing what you submitted and what you got back.

MS. OLSON: That's right --

MR. HUGHES: In the end you can always -- and there

is no -- I believe there is absolutely no technical way of avoiding that problem. That is an inherent part of this. If I have a list and I want to send a mail, and you want to tell me not to mail certain people on it, you have got to tell me who not to mail it to.

I guess one of the things I did see in your proposal that would be an option would be forcing everyone to forward all their mail through a gateway and yes, that could accomplish that, because then I don't know what's not getting through.

At the same time, then I kind of want to know what's not getting through. That's for a different reason that's important. And also, that I think is an even bigger technical problem.

(Several people speak simultaneously.)

MR. SALSBURG: For the court reporter's benefit, just one at a time.

MR. HUGHES: So, as a non-technologist, let me sort of recapture this in a way that makes sense to me, and maybe that will be helpful.

When we were talking about the two different visions, the two different possibilities that Peter was describing, what we were seeing in the RFI is the strong influence of the Do Not Call Registry, that the idea that a centralized database of e-mail addresses that would be sort

of a global suppression list for all of the senders in the world to use, that that thematically seems to emerge.

And the more we talked about it, the more we realized that there are both public policy concerns and then just channel differences between e-mail and telephones that led us to a discussion of more distributed models.

And whether you call it a Do Not E-Mail Registry, or you just say it's compliance with the CAN-SPAM Act, I think the vision that we're trying to describe with this distributed idea is not a centralized database, a database of suppressed names.

Because e-mail is so much more complex than telemarketing, the transactional messages, the newsletters, and all the different types of things that get communicated through e-mail.

But rather, CAN-SPAM gives us an architecture, a vision of how suppression should occur. And lo and behold, that vision is being realized in the marketplace today. And with some overlays on top of that sort of distributed un-sub process, distributed suppression list process that is occurring today, we may be able to call something a Do Not E-Mail -- don't call it a registry, but a Do Not E-Mail -- function, but that is distributed and is entirely consistent and dovetails with CAN-SPAM as it stands –

MR. SALSBURG: Well, let me see if I understand.

There are a couple of models of distributed Do Not E-Mail Lists that are being described. One was I would go to central authority, register my address. My address would then be sent to my ISP. AOL would be informed that I'm unsubscribing?

MS. OLSON: Well, no. Actually what I think you would do is AOL would have -- would register unsubs with some trusted -- I guess they're global unsubs, but some trusted party, right? There would be some number of those services.

MR. BAER: Or AOL might do their own --

MS. OLSON: Some company --

MR. BAER: There is always that possibility.

MR. BRONDMO: Can I -- I think we're missing the distributed model a little bit. If we assume there is authentication, so we know the mail is coming from where it says it's coming from, and we assume that there is a service -- say that there is one or more accreditation service, what does accreditation do?

Accreditation essentially categorizes or classifies the mail. So, I might get accredited to send unsolicited commercial e-mail from unsolicited.gap.com. And that domain has been accredited.

So, when you get a mail from unsolicited.gap.com you know it's unsolicited mail. So if anybody receiving mail from that domain does not want unsolicited commercial e-mail,

they have to set their filter or tell their ISP that they don't want unsolicited mail. That's the distributed model.

So what it says -- it flips the whole thing around, and it says with accreditation, a domain is now categorized to send a certain -- or the market place will determine what types of mail a certain -- you know, can do what.

So, you might have -- if you're Gap, you might have 10 domains, sub-domains. So you have Gap.com, and then for the purposes of e-mail you have -- you know, if you don't want to call it unsolicited you can call it offers.gap.com -- you will call it newsletter.gap.com, you will call it purchasereceipts.gap.com, loyaltycardsstatements.gap.com. You know, the only thing you can send from each one of those domains -- remember, we have authenticated the domains, so we know the mail is coming from that domain -- the only thing you can send within your accreditation and remain accredited is what those things say.

So, now I can step back in the distributor model. I don't need a centralized registry, because I can say, "I don't want mail that has not been authenticated, I don't want mail that is unsolicited mail, all I want is stuff that I have given explicit permission," which would be part of the accreditation. That would be a domain which is optin.gap.com.

So all I get is the mail that the network -- that

meets a certain set of criteria. And those criteria can be set up at my desktop, they can be set up at the perimeter. So, in other words, my corporate mail guys can set it up. Or, by my ISP -- Yahoo! or Hotmail -- they can set it up. And so --

MR. HUGHES: Or they could be shipped back out to that sender to be put on a suppress list of that sender, as well.

MR. BRONDMO: They could be shipped out, but I don't necessarily see that as being necessary in this model, and that's why I think it's significantly more secure.

So now, if I am, you know, me@earthlink, and I want to stop all unsolicited mail, what I would do in this scenario is I would say, "Unless mail is authenticated, I don't want it, or unless it's trusted source." So I would say, "Unless it's trusted, I don't want it." And -- or drop anything that's not trusted into a folder and find how many e-mails got into that folder every day so I can go look through them and if I need to dig something out -- but basically, if it's not trusted, I don't want it.

And if it's unsolicited, if I didn't explicitly solicit a commercial, if it's an unsolicited ad or commercial, I don't want it. And purchase receipts would not, for instance, be in that category.

And then, since you know what the incoming mail is

-- it's also like you have, you know, somebody sitting in the front office looking at stuff coming in. You know, they occasionally get those envelopes where you don't quite know what's in them, and you have to open them because it might be something important but, you know, they trick you that way.

Well, that won't be possible, because on the front there will be -- you know, you will be able to call somebody up to say, "Hey, look, there is a special code on this thing. What's in the envelope?" And you know, it will tell you what's in it, and whether they have a good reputation or not, and you will set it aside and sort it accordingly.

MR. SALSBURG: So what you're proposing isn't really a Registry, it's Project Lumos.

MR. BRONDMO: Well, it's not Project Lumos, per se, but it is that -- the architecture that we have proposed in Project Lumos, which is a distributed architecture where there is accountability in the network, and where you're held accountable for the mail you're sending, and therefore the recipient can make a choice as to whether to receive or not.

So, it is a distributed model for Do Not E-Mail which says I can determine all the way down to my desktop, I can determine whether I want your e-mail or not, or whether I want a class or a type of e-mail or not. So there is a distributed model as opposed to this one centralized --

MR. SALSBURG: So, conceptually, the idea is that

consumers have the choice of whether or not to get many types of e-mail, and this would provide --

MR. HUGHES: And they can segment it on a number of different -- by sender, by category, or classification of e-mail, or a number of different ways, and then --

MR. BRONDMO: -- determine what those categories are.

MR. HUGHES: But you know, we didn't mean for this to be a Project Lumos session. What we wanted to share was that these types of solutions that we're describing, the authentication piece is really, really close. The authentication piece on top of the authentication piece is sort of on the horizon, and there is some very good organizations working on it right now. It is emerging.

And the combination of those, we think, leads to a really powerful solution. As regards to Do Not E-Mail, we think that those solutions actually offer some intriguing possibilities with Do Not E-Mail. And some ways to rethink Do Not E-Mail so as to have the same effect or even more effect than you would with the centralized e-mail model.

But at the end of the day, what we want to offer and want to be here for is to really show that there is enormous technological data, and really good thinking going into solutions to spam and consumer tools that will really help, and we would love to make those available to you as

you're going through your proposals that you get back from your RFI. The depth from our Technology Committee really could help.

MS. OLSON: Yes, because I think what you're hearing is that, you know, we spent some time looking at this problem and we have thought of -- you know, there are a bunch of potential solutions to Do Not E-Mail that would work, depending on how strict your definition of Do Not E-Mail is exactly as, say, the -- exactly how strict your definition of it is, as a list or are you focused, you know, on a sort of more high-level definition of it, of solving the consumer's problems.

There are a bunch of different ways that you could solve it, and some of what you have heard is that variety -- you know, from the four of us describing different things is that variety of doing it, and there are advantages and flaws and features to all of them, just like there always are with a technical solution.

MR. MESNIK: We can certainly provide you more thorough information about some of the ideas that we have presented, all of this underlying structure. We're going to fix that, right? And then on top of that is, you know, the government's desire to have a Do Not E-Mail List, a concept. And there is ways in which you can actually layer that concept on top of all the things that we're already doing and

effectively achieve some of those very same goals.

MR. BAER: But Lumos isn't the answer, and we're not trying to come through with the answer at all, and so sometimes some of the questions you're asking are like, "Well, is that the answer?"

And like, it's hard to -- you know, we don't claim to have all the answers. We think we have a lot of good feedback involved in trying to help evaluate those answers.

MR. SALSBURG: You shouldn't read anything into the questions that we ask.

(Laughter.)

(Several people speak simultaneously.)

MR. BAER: Because here is a vision, you know, here is a way that we can move towards spurring a lot of discussion.

MR. HUGHES: So, is -- so we can wrap up any time you want, that's fine. But you know, bottom line, we just wanted to make sure that you knew we were available to continue talking --

MR. SALSBURG: I appreciate it. This has been very enlightening.

MS. ROBBINS: Yes.

MR. SALSBURG: So thank you for taking the time to come in and speak with us. And we very well may give you a call, Trevor, and --

MR. HUGHES: What's the timeline, now? I know the deadline is tomorrow for our responses.

MR. SALSBURG: Right.

MR. HUGHES: And then what's the timeline for you sort of packaging your report?

MR. SALSBURG: Well, the report is due in Congress on June 16th. And internally, that means that the draft will be prepared far in advance of that so the Commissioners can all read it and --

MR. HUGHES: Vote on it?

MR. SALSBURG: Vote on it. So we're looking at a pretty busy next six weeks of late nights.

MR. HUGHES: Okay.

MS. BUSH: I would just like to say regarding the reward system proposal, obviously we haven't had a chance to talk about it today, but it's Section 11.1 of the CAN-SPAM Act. I have, I think, five copies of that relevant Section for this, if you would like to take them.

MR. HUGHES: Great.

MS. BUSH: And then beyond that, you can e-mail me.

MR. HUGHES: Would you like us to come back in?

MS. BUSH: Well --

MR. HUGHES: We would like to talk to you more about it.

MS. BUSH: Okay. If you have ideas, and you would

like to schedule a session, that's something you could do. We have also put out a Request for Comments and the AMPR will be coming out shortly.

MR. HUGHES: When is that coming up?

MS. BUSH: I don't know yet.

MR. SALSBURG: I don't know if it's approved.

MR. HUGHES: We've been waiting with baited breath.

MS. BUSH: Well, again, yes. I don't know the specifics of that, but there will be some questions coming out about it. If you have things to say that you would like to do in person, we would be happy to do that as well.

MR. HUGHES: Okay.

MS. BUSH: So please feel free to get in touch with me about that.

MR. HUGHES: Excellent.

MR. SALSBURG: Thank you again, so much.

(Whereupon, at 12:27 p.m., the morning session was adjourned.)

C E R T I F I C A T I O N O F R E P O R T E R

DOCKET/FILE NUMBER: P044405

CASE TITLE: DO NOT E-MAIL REGISTRY MEETING

DATE: MARCH 9, 2004

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the tapes transcribed by me on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: MARCH 15, 2004

LISA SIRARD

C E R T I F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

SARA J. VANCE